Bobby Saadian, SBN 250377
bobby@wilshirelawfirm.com
Justin F. Marquez, SBN 262417
justin@wilshirelawfirm.com
Thiago M. Coelho, SBN 324715
thiago@wilshirelawfirm.com
Robert J. Dart, SBN 264060
rdart@wilshirelawfirm.com
Patty W. Chen, SBN 322992
patty@wilshirelawfirm.com
WILSHIRE LAW FIRM
3055 Wilshire Blvd., 12th Floor
Los Angeles, California 90010
Telephone: (213) 381-9988
Facsimile: (213) 381-9989

Attorneys for Plaintiffs and the Putative Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

ROBIN AMAN; ZIGMUND CAPULONG; and BELLS HAKALA, individually and on behalf of all others similarly situated. Plaintiffs, v. BAMBOO HR, LLC, a Utah limited liability company, BAMBOOHR PAYROLL, LLC, a Utah limited liability company; and DOES 1 to 10, inclusive, Defendants.	CASE NO.: **CLASS ACTION** **COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs Robin Aman, Zigmund Capulong, and Bells Hakala ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this action based upon their personal knowledge as to themselves and their own acts, and as to all other matters upon information and belief, based upon, *inter alia*, the investigation of their attorneys.

/ / /

/ / /

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

NATURE OF THE ACTION

1. Defendants Bamboo HR LLC and BambooHR Payroll LLC (collectively "Defendants" OR "Bamboo") provide human resources and payroll solutions to small and medium sized businesses. Bamboo's clients provide Bamboo with the highly sensitive personal information of those clients' employees, including addresses, phone numbers, social security numbers, and direct deposit banking information, and Bamboo provides human resources software solutions and payroll services for those clients. Those employees expect, when they provide this highly sensitive personal information to their employers, that it will be handled with care by any third parties with whom those employers contract for human resources or payroll services. What these employees do not expect, and did not expect, was that their personal and sensitive information would be harvested by unauthorized individuals.

2. Plaintiffs, individually and on behalf of those similarly situated persons (hereafter, "Class Members"), bring this class action to secure redress against Defendants for their reckless and negligent violation of their privacy rights. Plaintiffs and Class Members are individuals whose employers contracted with Bamboo for human resources and payroll services and were subject to a data breach.

3. Plaintiffs and Class Members suffered significant injuries and damages. The security breach compromised the full names, social security numbers, states of residence, states of employment, wage types, applicable tax codes, and other private identifiable information (referred to collectively as "PII") of the employees.

4. As a result of Defendants' wrongful actions and inactions, unauthorized individuals gained access to and harvested Plaintiffs' and Class Members' PII. Plaintiffs and the Class Members have been forced to take remedial steps to protect themselves from future loss. Indeed, all Class Members are currently at a very high risk of identity theft and/or credit fraud, and prophylactic measures, such as the purchase of credit monitoring, are reasonable and necessary to prevent and mitigate future loss.

5. As a result of Defendants' wrongful actions and inactions, employee information was stolen. Many employees who were included in Bamboo's database have had their PII

compromised, have had their privacy rights violated, have been exposed to the risk of fraud and identify theft, and have otherwise suffered damages.

THE PARTIES

6. Plaintiff Robin Aman is a California citizen residing in Sacramento, California. Plaintiff Zigmund Capulong is a California citizen residing in San Pedro, California. Plaintiff Bells Hakala is a California citizen residing in San Luis Obispo, California. Plaintiffs are each employees of companies which contracted with Bamboo for payroll services and whose PII was provided by their employers to Bamboo pursuant to those services. Plaintiffs' employers entered contracts with Bamboo which incorporated a contractually binding privacy policy for which Plaintiffs were intended third-party beneficiaries. Plaintiffs are informed and believe that, as a result of the data breach that took place at Bamboo, Plaintiffs' PII was accessed by hackers. As a result, Plaintiffs have to purchase credit and personal identity monitoring service to alert them to potential misappropriation of their identities and to combat risk of further identity theft. At a minimum, therefore, Plaintiffs have suffered compensable damages because they will be forced to incur the cost of a monitoring service, which is a reasonable and necessary prophylactic step to prevent and mitigate future loss. Exposure of Plaintiffs' PII as a result of the Bamboo data breach has placed them at imminent, immediate and continuing risk of further identity theft-related harm.

7. Defendant Bamboo HR LLC is a Utah limited liability company headquartered in Lindon, Utah, and with a California office located at 740 Alfred Nobel Drive, Hercules, CA 94547.

8. Defendant BambooHR Payroll LLC is a Utah limited liability company headquartered in Lindon, Utah, and with a California office located at 740 Alfred Nobel Drive, Hercules, CA 94547.

9. Plaintiffs are unaware of the true names, identities, and capacities of the defendants sued herein as DOES 1 to 10. Plaintiffs will seek leave to amend this complaint to allege the true names and capacities of DOES 1 to 10 if and when ascertained. Plaintiffs are informed and believe, and thereupon allege, that each of the defendants sued herein as a DOE is

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

legally responsible in some manner for the events and happenings alleged herein and that each of the defendants sued herein as a DOE proximately caused injuries and damages to Plaintiffs and Class Members as set forth below.

10. As used herein, "Defendants" shall refer to Bamboo and Does 1 to 10, collectively.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over the claims asserted herein pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), since some of the Class Members are citizens of a State different from the Defendant, there are more than 100 putative class members, and the amount in controversy exceeds $5 million.

12. The Court has personal jurisdiction over Defendants because Plaintiffs' and Class Members' claims arise out Defendants' business activities conducted in the State of California and through its interactive website through which it conducts business with California citizens.

13. Venue is appropriate in this District because, among other things: (a) Defendants maintain offices in this District, where they conduct substantial business; (b) Defendants directed their activities at residents in this District; and (c) many of the acts and omissions that give rise to this Action took place in this judicial District.

14. Venue is further appropriate in this District pursuant to 28 U.S.C. § 1391 because Defendants conduct a large amount of their business in this District, and because Defendants have substantial relationships in this District.

FACTUAL ALLEGATIONS

A. Bamboo's Data Breach

15. Defendants Bamboo provide human resources and payroll solutions to small and medium sized businesses throughout the country. In March, 2019, Defendants announced that "[o]n February 13, 2019, BambooHR became aware of unauthorized access by an unidentified third-party to the TraxPayroll system," and that "a report was accessed that may have allowed the third party to view personal information of certain employees." The notice issued by Defendants states that the information acquired included "the names, social security numbers, states of

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

residence, states of employment, wage types, and applicable tax type codes of certain employees." Notice of Data Breach attached hereto as **Exhibit A**.

16. Defendants made repeated promises and representations to their clients, which formed a part of their contracts with those clients, that they would protect Plaintiffs and the Class Members' PII from disclosure to third parties, including taking appropriate steps to safeguard their electronic databases. Plaintiffs and the Class Members were the intended third party beneficiaries of those promises since it was their PII, and not their employers', which was being safeguarded and since it was Plaintiffs and the Class Members, and not their employers, who would suffer the consequences of a data breach. A motivating purpose of the promise to protect Plaintiffs' and the Class Members' PII was thus to provide the benefit of data security to Plaintiffs and the Class Members. Further, permitting Plaintiffs and the Class Members to bring their own breach of contract action here is consistent with the objectives of the contract and the reasonable expectations of the contracting parties because, as the employers cannot sue Defendants for disclosing their employees' PII, there is no way for Plaintiffs and the Class Members to obtain redress for the breach of contract without allowing them to sue on their own behalf.

17. Defendants promised that they would not disclose Plaintiffs' and the Class Members' PII to any unauthorized third parties. In fact, they allowed hackers to obtain it.

B. Defendants Had an Obligation to Protect Personal Information under Federal Law.

18. Defendants are prohibited by the Federal Trade Commission Act (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission has found that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the Federal Trade Commission Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 243 (3d Cir. 2015).

C. California Recognizes the Importance of PII

19. California Civil Code § 1798.81.5(a)(1) states that: "It is the intent of the Legislature to ensure that personal information about California residents is protected. To that

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information."

D. Applicable Standards of Care

20. In addition to their obligations under federal and state laws, Defendants owed a duty to Plaintiffs and the Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to Plaintiffs and the Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems and networks, and the personnel responsible for them, adequately protected the PII of Plaintiffs and the Class Members.

21. Defendants owed a duty to Plaintiffs and the Class Members to design, maintain, and test their computer system to ensure that the PII in Defendants' possession was adequately secured and protected.

22. Defendants owed a duty to Plaintiffs and the Class Members to create and implement reasonable data security practices and procedures to protect the PII in their possession, including adequately training their employees and others who accessed PII within their computer systems on how to adequately protect PII.

23. Defendants owed a duty to Plaintiffs and the Class Members to implement processes that would detect a breach of their data security systems in a timely manner.

24. Defendants owed a duty to Plaintiffs and the Class Members to act upon data security warnings and alerts in a timely fashion.

25. Defendants owed a duty to Plaintiffs and the Class Members to disclose if their computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to purchase services from Defendants or to entrust PII with Defendants.

26. Defendants owed a duty to Plaintiffs and the Class Members to disclose in a timely and accurate manner when data breaches occurred.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

27. Defendants owed a duty of care to Plaintiffs and the Class Members because they were foreseeable and probable victims of any inadequate data security practices. Defendants collected Plaintiffs' and the Class Members' PII. Defendants knew that a breach of its data systems would cause Plaintiffs and the Class Members to incur damages.

E. Stolen Information Is Valuable to Hackers and Thieves

28. It is well known, and the subject of many media reports, that PII is highly coveted and a frequent target of hackers. Especially in the technology industry, the issue of data security and threats thereto is well known. Despite well-publicized litigation and frequent public announcements of data breaches, Defendants maintained an insufficient and inadequate system to protect the PII of Plaintiffs and Class Members.

29. Legitimate organizations and members of the criminal underground alike recognize the value of PII. Otherwise, they would not aggressively seek and pay for it. As previously seen in one of the world's largest data breaches, hackers compromised the card holder data of 40 million of Target's customers. *See* "Target: 40 million credit cards compromised," CNN Money, Dec. 19, 2013, *available* at http://money.cnn.com/2013/12/18/news/companies/target-credit-card/. DataCoup is, in contrast, just one example of a legitimate business that pays users for personal information. *See* http://money.com/money/3001361/datacoup-facebook-personal-data-privacy/.

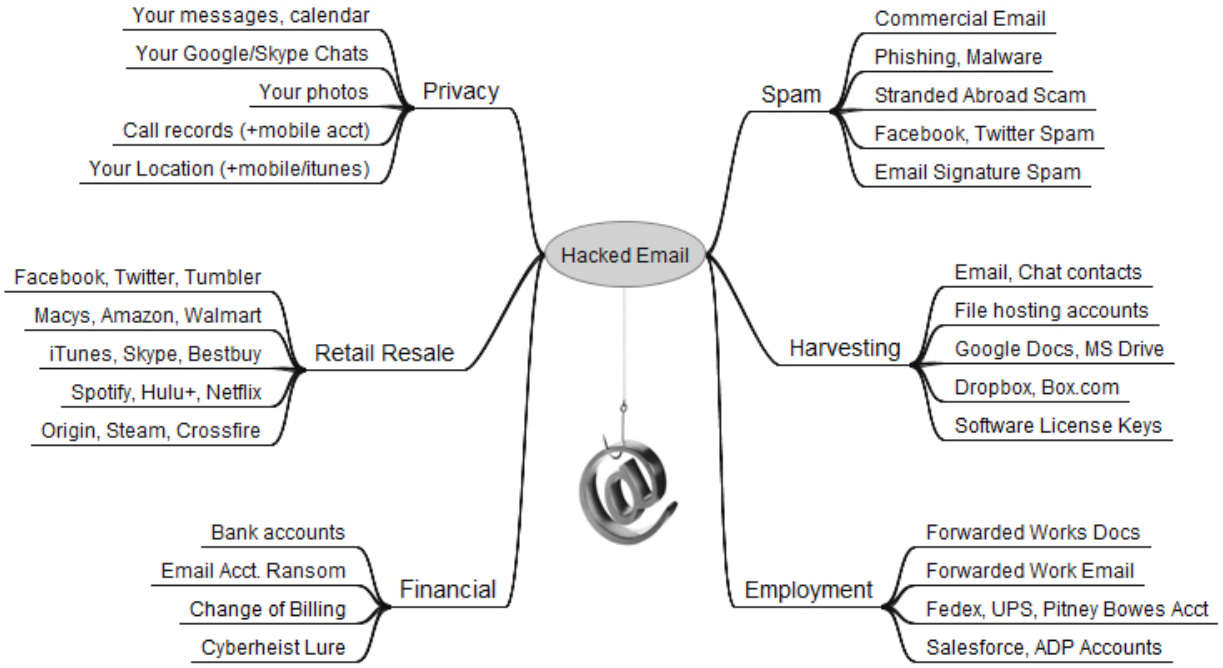
30. PII is highly valuable to hackers. Identity thieves use stolen PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. PII that is stolen from the point of sale are known as "dumps." *See* Krebs on Security April 16, 2016, Blog Post, *available at* https://krebsonsecurity.com/2016/04/all-about-fraud-how-crooks-get-the-cvv/. PII can be used to clone a debit or credit card. *Id.*

31. Once someone buys PII, it is then used to gain access to different areas of the victim's digital life, including bank accounts, social media, and credit card details. During that process, other sensitive data may be harvested from the victim's accounts, as well as from those belonging to family, friends, and colleagues.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

32. In addition to PII, a hacked email account can be very valuable to cyber criminals. Since most online accounts require an email address not only as a username, but also as a way to verify accounts and reset passwords, a hacked email account could open up a number of other accounts to an attacker.[1]

33. As shown below, a hacked email account can be used to link to many other sources of information for an identity thief, including any purchase or account information found in the hacked email account.[2]



34. Hacked information can also enable thieves to obtain other personal information through "phishing." According to the Report on Phishing available on the United States, Department of Justice's website: "AT&T, a large telecommunications company, had its sales system hacked into, resulting in stolen order information including full names and home addresses, order numbers and credit card numbers. The hackers then sent each customer a highly personalized e-mail indicating that there had been a problem processing their order and re-

[1] Identity Theft and the Value of Your Personal Data, Trend Micro (Apr. 30, 2015), https://www.trendmicro.com/vinfo/us/security/news/online-privacy/identity-theft-and-the-value-of-your-personal-data.

[2] Brian Krebs, The Value of a Hacked Email Account, Krebs on Security (June 13, 2013, 3:14 PM), https://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

directing them to a spoofed website where they were prompted to enter further information, including birthdates and Social Security numbers."[3]

D. The Data Breach Has Resulted and Will Result in Identity Theft and Identity Fraud

35. Defendants failed to implement and maintain reasonable security procedures and practices appropriate to protect the PII of Plaintiffs and Class Members.

36. The ramifications of Defendants' failure to keep Plaintiffs' and Class Members' PII secure is severe. According to Javelin Strategy and Research, "one in every three people who is notified of being a potential fraud victim becomes one . . . with 46% of consumers who had cards breached becoming fraud victims that same year." "Someone Became an Identity Theft Victim Every 2 Seconds Last Year," Fox Business, Feb. 5, 2014 *available* at http://www.foxbusiness.com/ personal-finance/2014/02/05/someone-became-identitytheft-victim-every-2-seconds-last-year.html.

37. In the case of a data breach, simply reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems." *See* "Victims of Identity Theft," U.S. Department of Justice, Dec 2013, *available at* https://www.bjs.gov/content/pub/pdf/vit12.pdf. In fact, the BJS reported, "resolving the problems caused by identity theft [could] take more than a year for some victims." *Id*. at 11.

38. A person whose PII has been obtained and compromised may not know or experience the full extent of identity theft or fraud for years. It may take some time for the victim to become aware of the theft or fraud. In addition, a victim may not become aware of fraudulent charges when they are nominal, because typical fraud-prevention algorithms fail to capture such charges. Those charges may be repeated, over and over again, on a victim's account, without notice for years.

/ / /

/ / /

[3] https://www.justice.gov/archive/opa/docs/report_on_phishing.pdf

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

F. Annual Monetary Losses from Identity Theft are in the Billions of Dollars

39. According to the BJS, an estimated 17.6 million people were victims of one or more incidents of identity theft in 2014. Among identity theft victims, existing bank or credit card accounts were the most common types of misused information. *Id*.

40. Javelin Strategy and Research reports that losses from identity theft reached $21 billion in 2013. There may be a time lag between when harm occurs and when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO, Report to Congressional Requesters, at 33 (June 2007), *available* at http://www.gao.gov/new.items/d07737.pdf.

41. As a result of the data breach, Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiffs and Class Members are also subject to a higher risk of phishing and pharming where hackers exploit information, they already obtained in an effort to procure even more PII. Plaintiffs and Class Members are presently incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges incurred by them and the resulting loss of use of their credit and access to funds, whether or not such charges are ultimately reimbursed by the credit card companies. In addition, Plaintiffs and Class Members now run the risk of unauthorized individuals creating credit cards in their names, taking out loans in their names, and engaging in other fraudulent conduct using their identities.

G. Plaintiffs and Class Members Suffered Damages

42. The exposure of Plaintiffs' and Class Members' PII to unauthorized third-party hackers was a direct and proximate result of Defendants' failure to properly safeguard and protect Plaintiffs' and Class Members' PII from unauthorized access, use, and disclosure, as required by

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

their contracts, and state and federal law. The data breach was also a result of Defendants' failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class Members' PII in order to protect against reasonably foreseeable threats to the security or integrity of such information, also required by their contracts and state and federal law

43. Plaintiffs' and Class Members' PII is private and sensitive in nature and was inadequately protected by Defendants. Defendants did not obtain Plaintiffs' and Class Members' consent to disclose their PII as required by applicable law and industry standards.

44. As a direct and proximate result of Defendants' wrongful actions and inaction and the resulting data breach, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing risk of harm from identity theft and identity fraud, requiring them to take the time and effort to mitigate the actual and potential impact of the subject data breach on their lives by, among other things, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports and accounts for unauthorized activity.

45. Defendants' wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class Members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. The improper disclosure, compromising, and theft of their PII;

b. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of unauthorized third-party hackers and misused via the sale of Plaintiffs' and Class Members' information on the Internet black market;

c. The untimely and inadequate notification of the data breach;

d. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the data breach; and

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

e. Ascertainable losses in the form of deprivation of the value of their PII, for which there is a well-established national and international market;

CLASS ACTION ALLEGATIONS

46. Plaintiffs bring this action on their own behalf on behalf of all others similarly situated under Rule 23(a), (b)(2), (b)(3), and (c)(4) of the Federal Rules of Civil Procedure. The Class is divided into two Classes as follows:

> The California Class:
>
> All persons residing in the State of California whose Personal Identifying Information was maintained by Bamboo HR, LLC, or Bamboo Payroll, LLC, and was compromised as a result of the breach discovered by Bamboo HR, LLC, on or about February 13, 2019.
>
> The Nationwide Class:
>
> All persons residing in the United States of America whose Personal Identifying Information was maintained by Bamboo HR, LLC or Bamboo Payroll, LLC, and was compromised as a result of the breach discovered by Bamboo HR, LLC, on or about February 13, 2019.

47. Excluded from the Class are: (a) Defendants, including any entity in which any of the Defendants has a controlling interest, is a parent or a subsidiary of, or which is controlled by any of the Defendants; (b) the officers, directors, and legal representatives of Defendants; and (c) the judge and the court personnel in this case as well as any members of their immediate families. Plaintiffs reserve the right to amend the definition of the Class if discovery, further investigation and/or rulings by the Court dictate that it should be modified.

48. *Numerosity*. The members of the Class are so numerous that the joinder of all Class Members is impractical. While the exact number of Class Members is unknown to Plaintiffs at this time, given the number of companies which use Bamboo in the United States, it stands to reason that the number of Class Members is at least in the thousands. Class Members are readily identifiable from information and records in Defendants' possession, custody, or control, such as account information.

49. *Commonality and Predominance*. There are questions of law and fact common to Class Members, which predominate over any questions affecting only individual Class Members.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

These common questions of law and fact include, without limitation:

a. Whether Defendants owed a duty of care to Plaintiffs and Class Members with respect to the security of their PII;

b. What security measures must be implemented by Defendants to comply with their duty of care;

c. Whether Defendants met the duty of care owed to Plaintiffs and the Class Members with respect to the security of the PII;

d. Whether Defendants have a contractual obligation to Plaintiffs and Class Members as third-party beneficiaries to use reasonable security measures;

e. Whether Defendants have complied with any contractual obligation to use reasonable security measures;

f. What security measures must be implemented by Defendants to comply with their contractual obligations to use reasonable security measures;

g. Whether Defendants' acts and omissions described herein violated the Federal Trade Commission Act (15 U.S.C. § 45);

h. Whether Defendants' acts and omissions described herein violated California Civil Code § 1798.81.5(a)(1);

i. What security measures, if any, must be implemented by Defendants to comply with their contractual and statutory obligations;

j. The nature of the relief, including equitable relief, to which Plaintiffs and Class Members are entitled; and

k. Whether Plaintiffs and Class Members are entitled to damages, civil penalties and/or injunctive relief.

50. *Typicality*. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PII, like that of each of the other Class Members, was exposed and/or improperly disclosed by Defendants.

51. *Adequacy of Representation*. Plaintiffs will fairly and adequately represent and protect the interests of the Class Members. Plaintiffs have retained competent counsel

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

experienced in litigation of class actions, including consumer and data breach class actions, and Plaintiffs intend to prosecute this action vigorously. Plaintiffs and Class Members have a unified and non-conflicting interest in pursuing the same claims and obtaining the same relief. Therefore, all Class Members will be fairly and adequately represented by Plaintiffs and their counsel.

52. *Superiority of Class Action*. A class action is superior to other available methods for the fair and efficient adjudication of the claims alleged in this action. The adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudications of the asserted claims. There will be no difficulty in the management of this action as a class action, and the disposition of the claims of the Class Members in a single action will provide substantial benefits to all parties and to the Court. Damages for any individual Class Member are likely insufficient to justify the cost of individual litigation so that, in the absence of class treatment, Defendants' violations of law inflicting substantial damages in the aggregate would go un-remedied.

53. Class certification is also appropriate because Defendants have acted or refused to act on grounds generally applicable to the Class Members, such that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

FIRST CAUSE OF ACTION

(Breach of Express And/or Implied Contractual Promise on Behalf of Both Classes)

54. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 53, inclusive, of this Complaint as if set forth fully herein.

55. Defendants were parties to contracts with Plaintiffs' and the Class Members' employers, pursuant to which Defendants obtained Plaintiffs' and the Class Members' PII for the purposes of payroll and human resources activities.

56. Bamboo's Privacy Notice formed a part of its contracts with Plaintiffs' and the Class Members' employers. Under the Privacy Notice, Bamboo promised to maintain adequate safeguards to protect the PII from disclosure to unauthorized third parties, and also promised not to disclose the PII to unauthorized third parties.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

57. Plaintiffs and the Class Members were the intended third party beneficiaries of these promises since it was their PII, and not their employers', which was promised to be safeguarded and since it was Plaintiffs and the Class Members, and not their employers, who would suffer the consequences of a data breach. A motivating purpose of the promise to protect Plaintiffs' and the Class Members' PII was thus to provide the benefit of data security to Plaintiffs and the Class Members.

58. Further, permitting Plaintiffs and the Class Members to bring their own breach of contract action here is consistent with the objectives of the contract and the reasonable expectations of the contracting parties because, as the employers cannot sue Defendants for disclosing their employees' PII, there is no way for Plaintiffs and the Class Members to obtain redress for the breach of contract without allowing them to sue on their own behalf.

59. Accordingly, the Privacy Notice is contractually binding upon Defendants with regard to Plaintiffs and each of the Class members.

60. The Privacy Notice describes Defendants' contractual duty to safeguard and protect Plaintiffs' and the Class Members' PII. Specifically, Defendants promised to take appropriate steps to safeguard the PII from disclosure, and also promised not to disclose the PII to unauthorized third parties.

61. The contractual duty to protect and safeguard Plaintiffs' and the Class Members' PII, which Defendants promised to undertake, was, even apart from the language of the Privacy Notice, a term of the contract by operation of law under the Federal Trade Commission Act (15 U.S.C. § 45). Under applicable law, all laws in place at the time a contract is entered which are relevant to the subject matter of that contract become binding terms of the contract. Therefore, the FTCA also formed a contractual term in each of Defendant's contracts with Plaintiffs and the Class Members.

62. Finally, the promise to safeguard and protect Plaintiffs' and the Class Members' PII, and keep that PII from being accessed by third parties, was implied as a matter of law because Defendant and Plaintiffs' and the Class Members' employers entered their agreements with the expectation and implied mutual understanding that Defendant would strictly maintain the

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

confidentiality of the PII and safeguard it from theft or misuse.

63. Therefore, Plaintiffs and Class Members are third-party beneficiaries of the contracts between Defendants and Plaintiffs and the Class Members' employers in which Defendants agreed to: (a) implement and maintain reasonable security procedures to protect Plaintiffs' and Class Members' personal information from unauthorized access, destruction, use, modification, or disclosure; and (b) prevent unauthorized third parties from obtaining access to Plaintiffs' and Class Members' PII.

64. Plaintiffs and Class Members' employers would not have provided and entrusted the PII to Defendants in the absence of the proper security safeguards and the promise to keep their PII safe.

65. Plaintiffs' and Class Members' employers fully performed their obligations under their agreements with Defendants.

66. Defendants breached the contractual promises by failing to: (a) implement and maintain reasonable security procedures to protect Plaintiffs' and Class Members' PII from unauthorized access, destruction, use, modification, or disclosure; and (b) prevent unauthorized third parties from obtaining access to Plaintiffs' and Class Members' PII.

67. Plaintiffs and the Class Members' expectation was that their PII would be safeguarded and protected. Therefore, they agreed to employment terms, such as compensation, to which they would not have agreed had they known that their PII would not be protected. Further, due to the fact that their PII was not protected, Plaintiffs and the Class Members incurred losses associated with the loss of PII privacy, including theft, identity theft, and the risk of theft and identity theft, along with the necessity of cancelling credit cards and paying for additional protection through the market.

68. As a direct and proximate result of Defendants' breaches of the contractual promises alleged herein, Plaintiffs and Class Members sustained actual losses and damages in an amount according to proof at trial but in excess of the minimum jurisdictional requirement of this Court.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

SECOND CAUSE OF ACTION

(Breach of Covenant of Good Faith and Fair Dealing on Behalf of Both Classes)

69. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 68, inclusive, of this Complaint as if set forth fully herein.

70. Applicable law implies a covenant of good faith and fair dealing in every contract.

71. Plaintiffs and Class Members were the third-party beneficiaries of contracts between Plaintiffs' and the Class Members' employers and Defendants.

72. Plaintiffs' and Class Member's employers performed all of their duties under their agreements with Defendants.

73. All of the conditions required for Defendants' performance under the contracts have occurred.

74. Incorporated in the contracts as a matter of law was the covenant of good faith and fair dealing, which prevents a contracting party from engaging in conduct that frustrates the other party's rights to the benefits of the agreement. The implied covenant imposes on a contracting party not only the duty to refrain from acting in a manner that frustrates performance of the contract, but also the duty to do everything that the contract presupposes that the contracting party will do to accomplish its purposes.

75. Here the implied covenant of good faith and fair dealing required Defendants to safeguard and protect from disclosure to third parties the PII of Plaintiffs and the Class Members which was turned over to Defendants only for the purposes of performing or procuring professional services for Plaintiffs and the Class Members. Plaintiffs and the Class Members could not enjoy Defendant's services without the safeguarding and protection of the PII.

76. Defendants breached the covenant of good faith and fair dealing implied in their contracts with Plaintiffs and Class Members by engaging in the following conscious and deliberate acts: (a) failing to implement and maintain reasonable security procedures to protect Plaintiffs' and Class Members' PII from unauthorized access, destruction, use, modification, or disclosure; and (b) failing to ensure that unauthorized parties were not provided access to Plaintiffs' and Class Members' PII. Defendants' failure to protect the PII of Plaintiffs and Class

Members frustrated Plaintiffs' and the Class Members' rights to the benefit of their employers' bargains with Defendant, to enjoy the professional services of Defendant without incurring risks of property and identity theft.

77. Plaintiffs and Class Members have lost the benefit of Defendants' contract by having their PII compromised and have been placed at an imminent, immediate and continuing risk of identity theft-related harm.

78. As a direct and proximate result of Defendants' breach of the covenant of good faith and fair dealing, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

THIRD CAUSE OF ACTION

(Violation of California Business and Professions Code §17200 *et. seq*. on Behalf of the California Class)

79. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 78, inclusive, of this Complaint as if set forth fully herein.

80. By their actions and conduct as alleged herein, Defendants have committed one or more acts of unfair competition within the meaning of California Business and Professions Code § 17200 ("UCL") that constitute unfair, unlawful and/or fraudulent business practices as those terms are defined under California law.

81. Defendants' business practices are unfair under the UCL because Defendants have acted in a manner that is immoral, unethical, oppressive, unscrupulous and/or substantially injurious to Plaintiffs and the Class Members. The exposure of PII to third parties is substantially injurious because of the significant harm that can result to the customer at the hand of those third parties, and the protective measures that the customer must undertake as a direct result of this exposure. Further, the impact of the practice against Plaintiffs and the Class Members far outweighs any possible justification or motive on the part of Defendant. Plaintiffs and the Class Members could not reasonably have avoided this injury because they relied upon Defendant's promises to protect and safeguard the PII from disclosure, as all employees must when providing

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

PII is a condition of employment.

82. Defendants' failure to safeguard and protect Plaintiffs' and the Class Members' PII is violative of public policy as expressed in the Federal Trade Commission Act (15 U.S.C. § 45). The Federal Trade Commission has found that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the Federal Trade Commission Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 243 (3d Cir. 2015). Defendant's failures are also violative of public policy as expressed in California Civil Code § 1798.81.5(a)(1), which states that: "It is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information."

83. Defendants' business practices are also unfair because they significantly threaten or harm competition. Participation in today's credit economy is predicated on the security of the PII of the participants in that economy, in the sense that PII is an asset of the individual which, if lost to him or her, jeopardizes his or her very ability to maintain capital. Competitive economic activity cannot exist where PII goes unprotected.

84. Defendants' business practices are unlawful under the UCL because Defendants have violated the FTCA, 15 U.S.C. § 45, and California Civil Code § 1798.81.5(a)(1).

85. Defendants violated the FTCA and § 1798.81.5(a)(1) by: (a) failing to implement and maintain reasonable security procedures to protect Plaintiffs' and Class Members' PII from unauthorized access, destruction, use, modification, or disclosure; and (b) failing to ensure that unauthorized parties were not provided with access to Plaintiffs' and Class Members' PII.

86. Plaintiffs and the Class Members have suffered monetary injury in fact as a direct and proximate result of the acts of unfair competition committed by Defendants as alleged herein in an amount to be proven at trial but in excess of the minimum jurisdictional amount of this Court.

/ / /

/ / /

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

FOURTH CAUSE OF ACTION

(Negligence on Behalf of Both Classes)

87. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 86, inclusive, of this Complaint as if set forth fully herein.

88. As described above, Defendants owed Plaintiffs and the Class Members duties of care in the handling of PII, which duties included keeping that PII safe and preventing disclosure of that PII to all unauthorized third parties.

89. Additionally, Defendants had a duty to Plaintiffs and the Class Members to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and Class Members' PII as required by the Federal Trade Commission Act (15 U.S.C. § 45). This legal duty arises outside of any contractual, implied or express, responsibilities that Defendants had between Plaintiffs and Class Members, as it is "completely independent" of any contract.

90. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

91. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

92. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII in its stores obtained and stored, and the foreseeable consequences of a data breach at a company as large as Defendants', including, specifically, the damages that would result to Plaintiffs and Class members.

93. The harm that occurred as a result of the security breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and

avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Class Members.

94. Defendants' failure to comply with applicable laws and regulations constitutes negligence per se.

95. In addition to their obligations under state and federal law, Defendants owed a duty to Plaintiffs and the Class Members, who entrusted them with sensitive PII, to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to Plaintiffs and the Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems and networks, and the personnel responsible for them, adequately protected the PII of Plaintiffs and the Class Members.

96. Defendants owed a duty to Plaintiffs and the Class Members to design, maintain, and test their computer system to ensure that the PII in Defendants' possession was adequately secured and protected.

97. Defendants owed a duty to Plaintiffs and the Class Members to create and implement reasonable data security practices and procedures to protect the PII in their possession, including adequately training their employees and others who accessed PII within their computer systems on how to adequately protect PII.

98. Defendants owed a duty to Plaintiffs and the Class Members to implement processes that would detect a breach of their data security systems in a timely manner.

99. Defendants owed a duty to Plaintiffs and the Class Members to act upon data security warnings and alerts in a timely fashion.

100. Defendants owed a duty to Plaintiffs and the Class Members to disclose if their computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to pursue employment with Defendants' clients.

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

101. Defendants owed a duty to Plaintiffs and the Class Members to disclose in a timely and accurate manner when data breaches occurred.

102. Defendants owed a duty of care to Plaintiffs and the Class Members because they were foreseeable and probable victims of any inadequate data security practices. Defendants collected Plaintiffs' and the Class Members' PII. Defendants knew that a breach of its data systems would cause Plaintiffs and the Class Members to incur damages.

103. Defendants breached those duties of care by adopting inadequate safeguards to protect the PII, and, on information and belief, failing to adopt industry-wide standards in their supposed protection of the PII, resulting in the disclosure of the PII to unauthorized third parties.

104. As a direct and proximate result of Defendants' failure to adequately protect and safeguard the PII, Plaintiffs and the Class members suffered damages. Plaintiffs and the Class Members were damaged because their PII was accessed by third parties, resulting in increased risk of identity theft and theft of property, and for which Plaintiffs and the Class members were forced to adopt costly and time-consuming preventive and remediating efforts. Plaintiffs and the Class Members were also damaged in that they paid for Defendants' services in an amount that they would have refused to pay had they known that Defendants would not protect their PII. Plaintiffs and the Class Members accepted pricing terms which they would not have agreed to had they known that Defendants would not protect their PII.

105. Defendants acted with wanton disregard for the security of Plaintiffs' and the Class Members' PII. Defendants knew or should have known that Bamboo had inadequate computer systems and data security practices to safeguard such information, and Defendants knew or should have known that hackers were attempting to access the PII of employee databases, such as Bamboo's.

106. A "special relationship" exists between Defendants and Plaintiffs and the Class Members. Defendants entered into a "special relationship" with Plaintiffs and the Class Members when they contracted to provide Plaintiffs and the Class Members with HR and payroll services and obtained their PII from them. As the gatekeepers to Plaintiffs' and the Class Members' professional incomes, Defendants stand in a fiduciary or quasi-fiduciary relationship with

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137

Plaintiffs and the Class Members.

107. Furthermore, Defendants also created a "special relationship" with Plaintiffs and Class Members who provided their information to Defendants and their clients, by playing a large role in creating and maintaining centralized computer systems and data security practices that were used for storage of all of Defendants' clients' employees' PII.

108. Plaintiffs and the Class Members have suffered monetary injury in fact as a direct and proximate result of the acts of negligence committed by Defendants as alleged herein in an amount to be proven at trial but in excess of the minimum jurisdictional amount of this Court.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the Class, pray for relief as follows:

1. For compensatory damages in an amount according to proof at trial;

2. For restitutionary damages in an amount according to proof at trial;

3. For affirmative injunctive relief mandating that Defendants implement and maintain reasonable security procedures and practices to protect Plaintiffs' and Class Members' PII from unauthorized access, destruction, use, modification, or disclosure;

4. For costs of suit and litigation expenses;

5. For attorneys' fees under the common fund doctrine and all other applicable law; and

6. For such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and all others similarly situated, hereby demand a jury trial for all claims so triable.

Dated: June 6, 2019

Respectfully submitted,

WILSHIRE LAW FIRM
/s/ *Thiago M. Coelho*
Thiago M. Coelho
Justin F. Marquez
Robert Dart
Patty Chen

WILSHIRE LAW FIRM, PLC
3055 Wilshire Blvd, 12th Floor
Los Angeles, CA 90010-1137